NCCoE TLS Server Certificate Management

National Cybersecurity Center of Excellence

Industry Day

9/26/2019

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Welcome/Overview of NIST and the NCCoE

Kevin Stine

NCCoE

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Welcome and Overview

Emergency Procedures for NCCoE Visitors

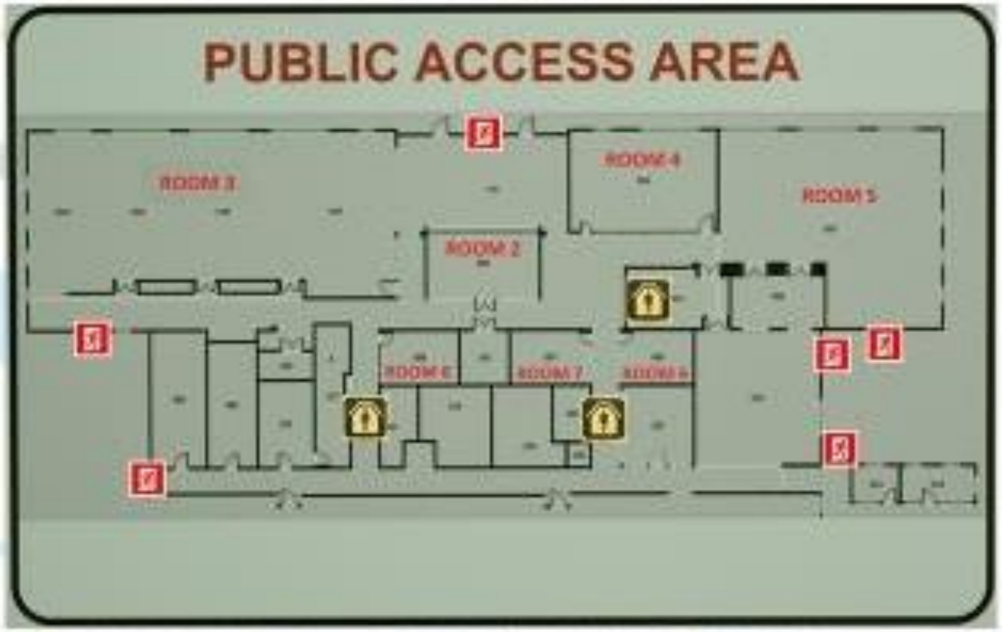
Evacuation Emergencies

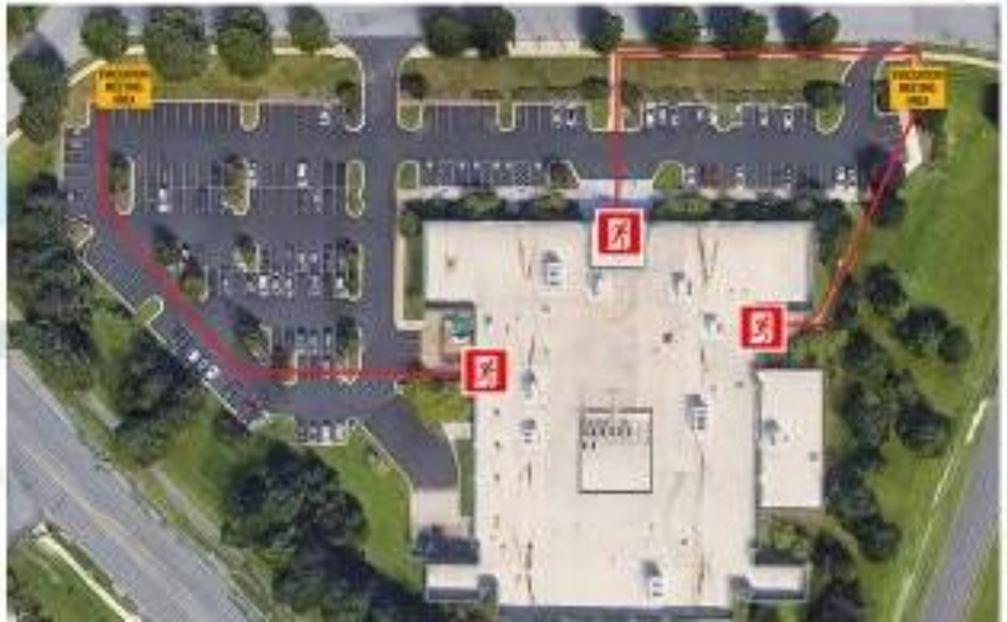
What is an Evacuation Emergency?

- Fires
- Explosions
- Earthquakes
- Indoor toxic material releases
- Indoor radiological and biological accidents
- Workplace violence

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest exit (Red Signs – **Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction
- Once outside the building, swiftly walk toward the designated meeting area near the posted sign stating "Evacuation Meeting Area" (Yellow Sign – **Lower Right Map**)





Shelter-In-Place (SIP) Emergencies

What is a Shelter-In-Place Emergency?

- Severe weather (hurricanes, tornadoes, etc.)
- chemical, biological, or radiological contaminants released into the environment

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest SIP hallway or room (Yellow Signs – **Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction

Agenda

8:30 – 9:00
Check-In

9:00 – 9:15
Welcome/Overview of NIST and the NCCoE
Kevin Stine

9:15 – 9:25
TLS Server Certificate Management Landscape – An Enterprise Perspective
Paul Turner

9:25 - 9:40
SP 1800-16 Practice Guide Overview
William C. Barker

9:40 - 9:45
Summary of Public Comments
Mary Raguso

9:45 – 10:30
Project Demonstration
Brett Pleasant, Mehwish Akram, and Brian Johnson

10:30 – 10:45
Break

10:55 – 11:15
SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security Implementations
Andrew Regenscheid

11:15 – 12:00
TLS Project Team Panel Discussion
Curt Barker, Rob Clatterbuck, Clint Wilson, Dung Lam, Jane Gilbert, and Paul Turner

12:00 – 12:30
Optional TLS Server Certificate Management Lab Tour

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

National Institute of Standards and Technology

National Institute of Standards and Technology

NIST is a bureau under the Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST runs a number of laboratories to assist in its mission.

Communications Technology Laboratory	Engineering Laboratory	Information Technology Laboratory	Material Measurement Laboratory	Physical Measurement Laboratory

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Introduction to NCCoE

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Introduction to NCCoE

NCCoE Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

NCCoE Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

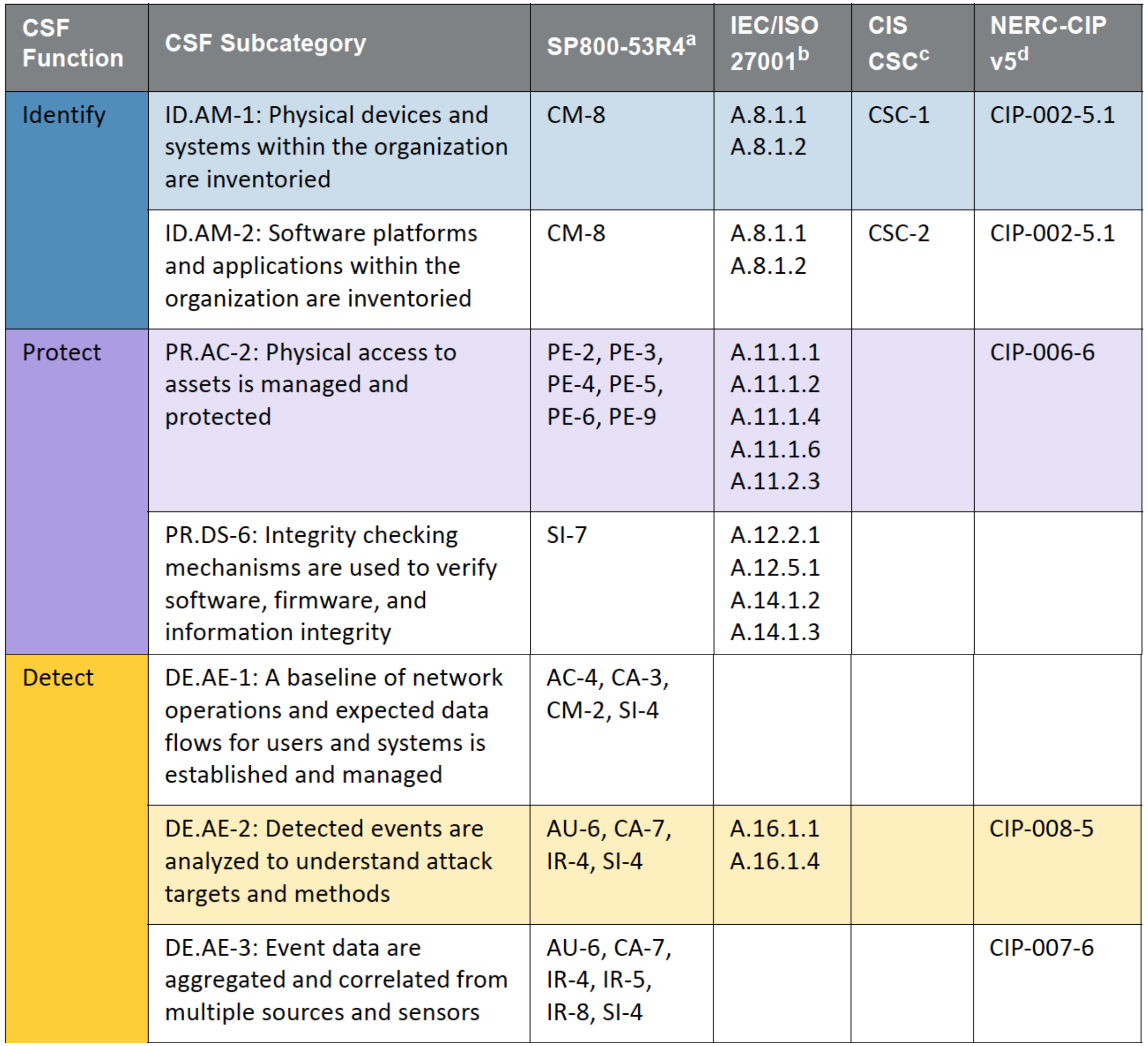
- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards

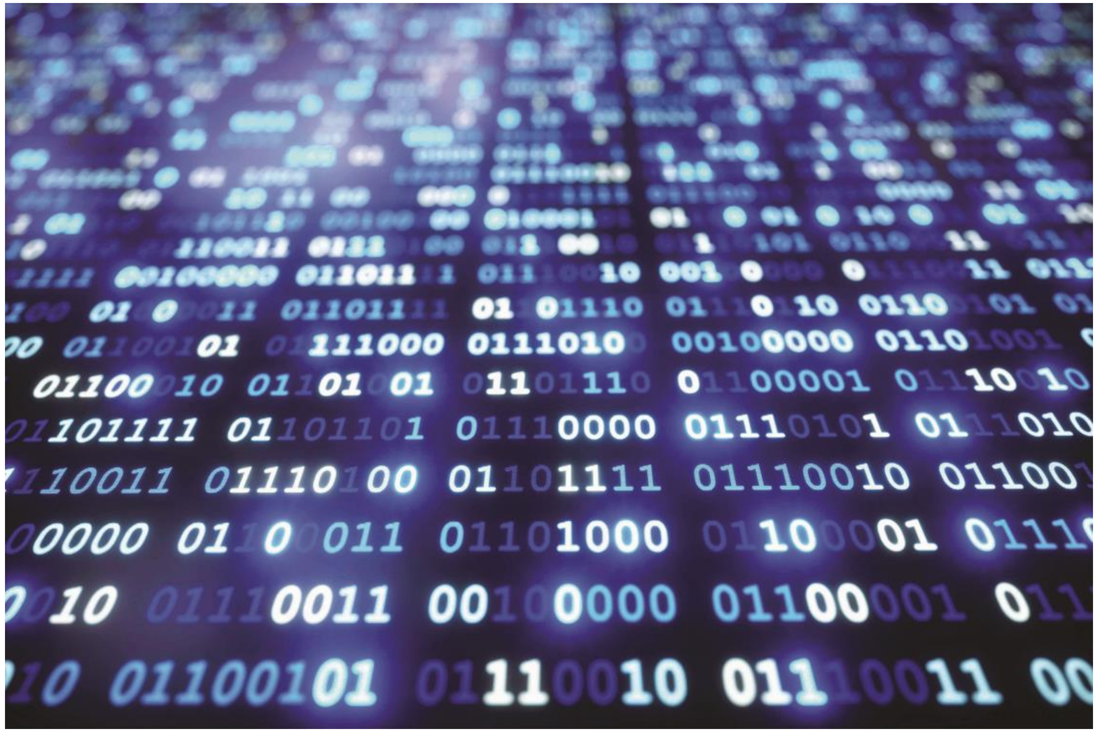
Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance



CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

Sector-Based Projects



Commerce/Retail (SP 1800-17)

Energy (SP 1800-2 & SP 1800-7)

Financial Services (SP 1800-5 & SP 1800-9 & SP 1800-18)

Healthcare (SP 1800-1 & SP 1800-8)

Hospitality

Manufacturing

Public Safety/First Responder (SP 1800-13)

Transportation

Cross-Sector Projects

- Attribute Based Access Control (SP 1800-3)
- Data Integrity (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Secured Email (SP 1800-6)
- Mitigating IoT-Based DDoS (SP 1800-15)
- Mobile Device Security (SP 1800-4 & SP 1800-21)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Management (SP 1800-16)
- Trusted Geolocation in the Cloud (SP 1800-19)

NCCoE

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Industry Day Purpose and Objectives

Purpose and Objectives of the Industry Day

Purpose

- NCCoE and industry collaborators, developed a draft practice guide SP 1800-16, for Securing Web Transactions
- Guide was developed to help medium and large enterprises oversee their TLS server certificates.
- Benefits Executives, Chief Information Security Officers, System Administrators, or anyone who has a stake in protecting his or her organization's data, privacy, and overall operational security.

Objectives

- Discuss the importance of having a TLS management plan
- The risks organizations face by not having a TLS management plan
- Demonstrate an example implementation of TLS certificate management in a typical enterprise organization using commercial off-the-shelf technologies
- Explain how the practice guide can aid your organization’s TLS management efforts

Attendees

172 people registered

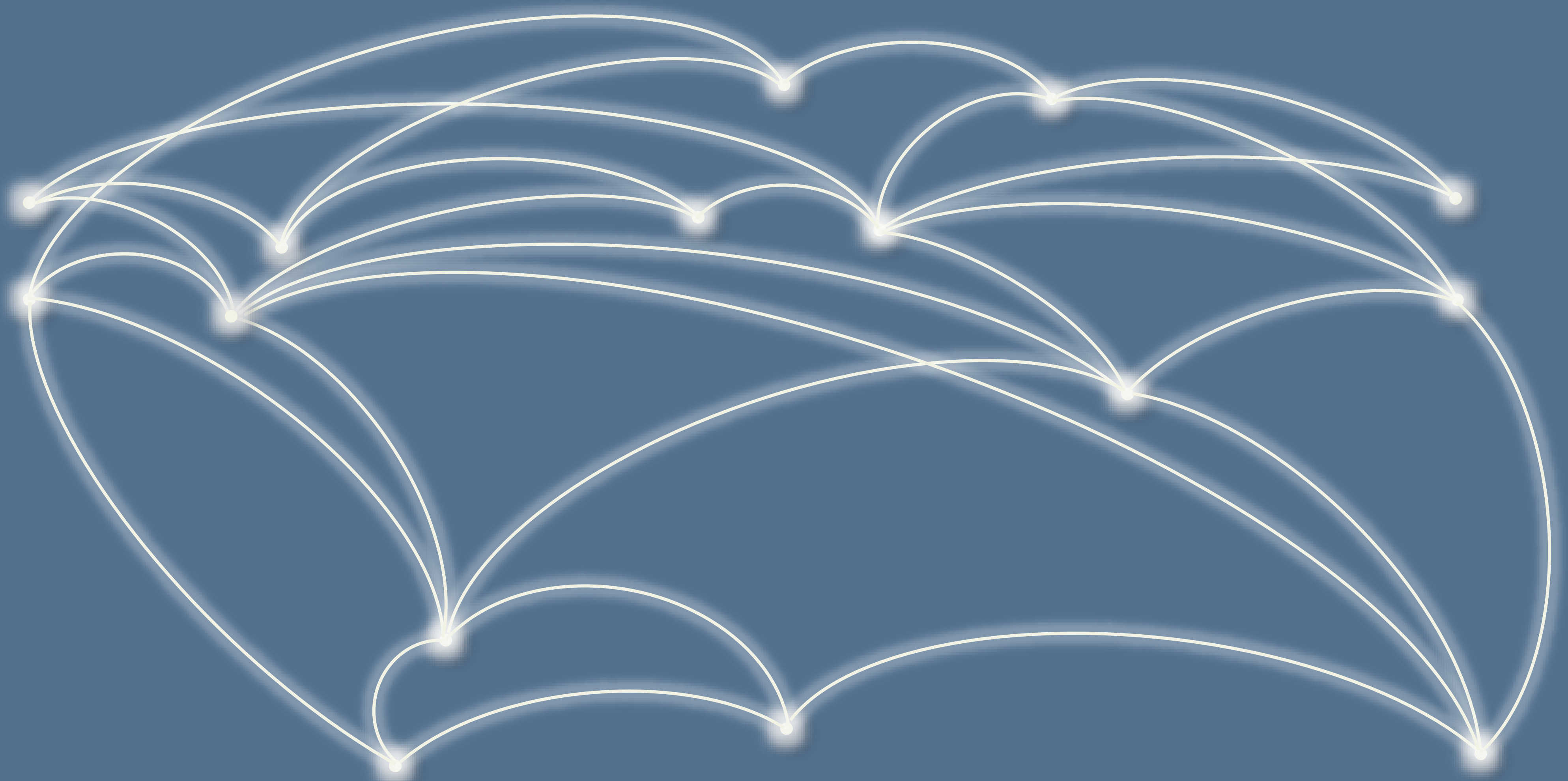
Registrants’ organizations breakdown:

- **Government—Federal, State, Local**
  - Newport News Public Schools; Department of Homeland Security, Clarksdale Public Utilities, Treasury, NOAA, Virginia Department of Education; Maryland Dept. of Corrections; NY Metro Infragard; U.S. Navy; NSA; FEMA
- **Academia**—Fordham University, Hagerstown Community College, Marymount; George Washington University
- **Private Industry**—Telecommunications; Banking; Healthcare, Banking; Hospitality; Aerospace; Management Consulting; Technology/IT; Insurance
- **Non-Profits/Not-for-Profits**—National Human Genome Research Institute; MITRE
- **Welcome to the Press!**

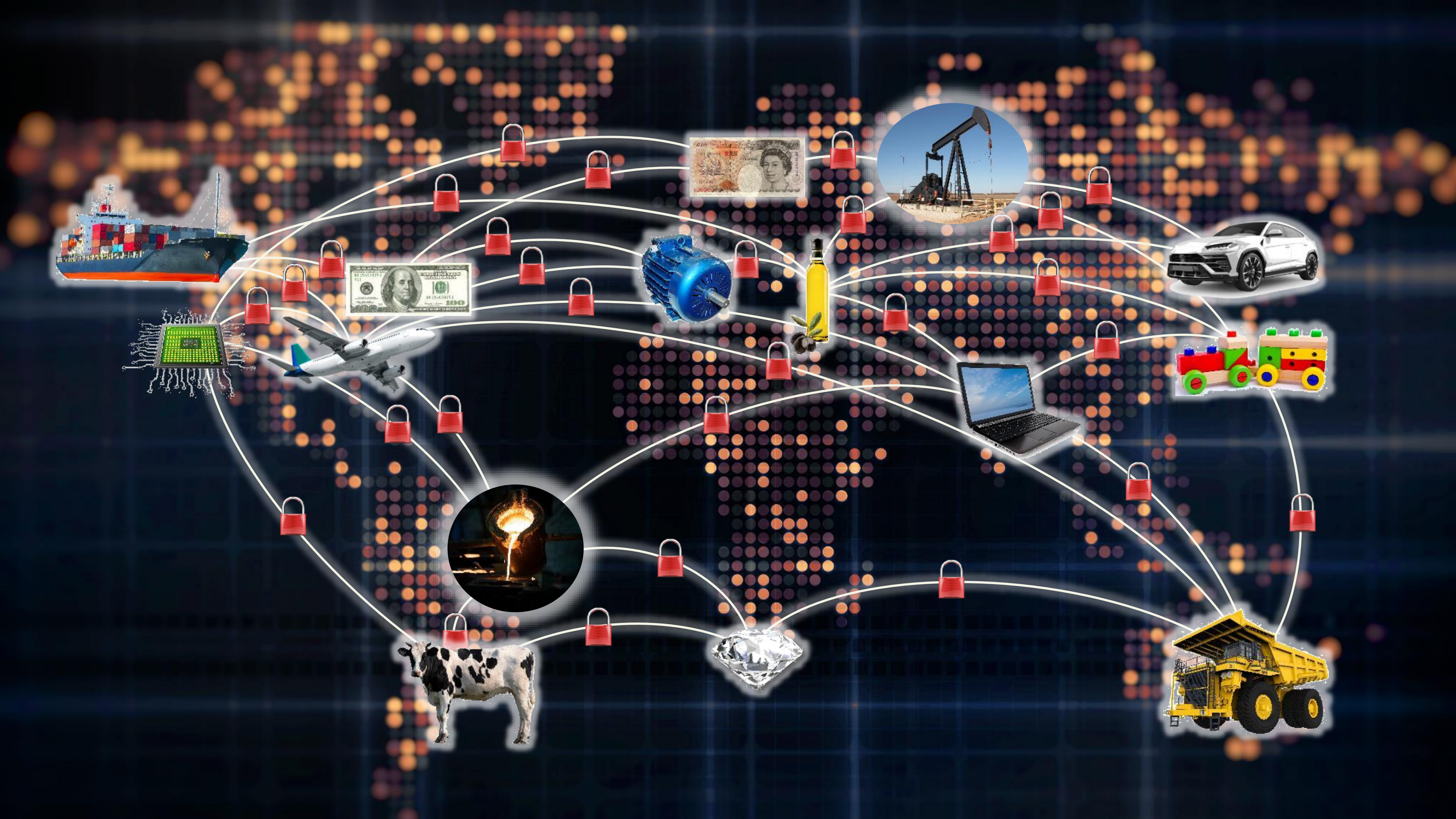
NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

TLS Cert Management Landscape – An Enterprise Perspective

Paul Turner



© 2019 Venafi. All rights reserved.

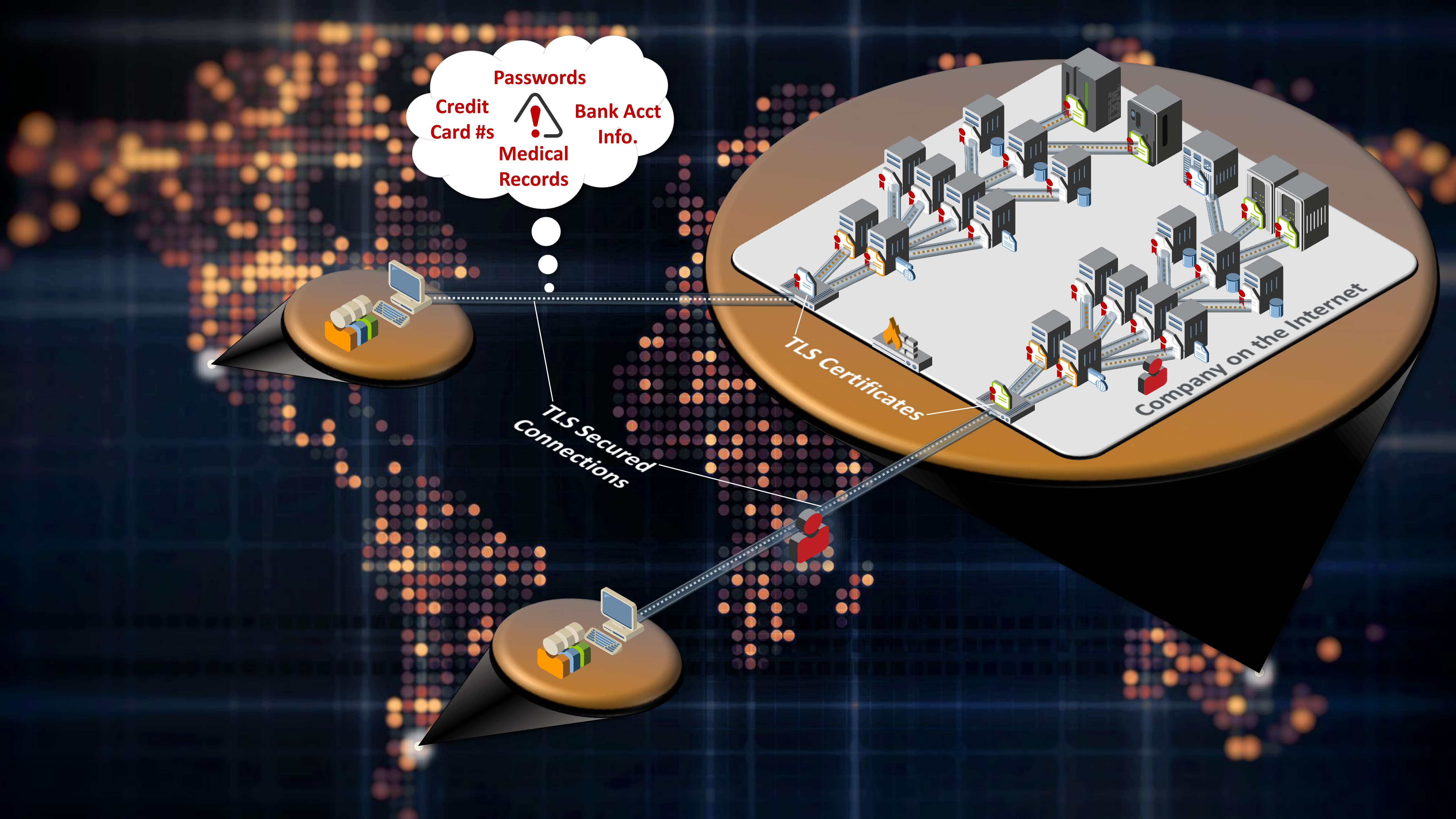


Authentication

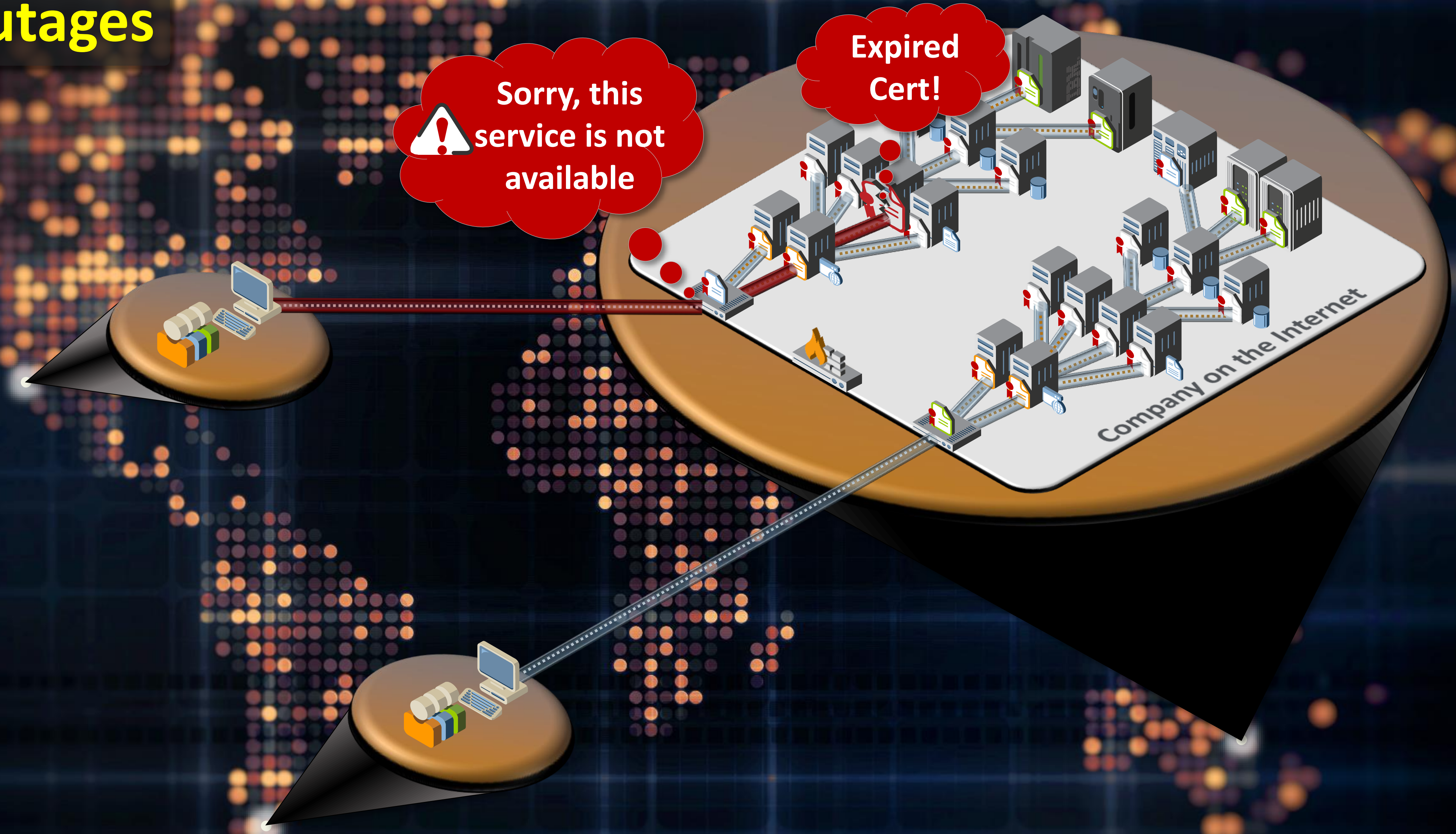
TLS

Transport Layer Security

Confidentiality


Passwords
Credit Card #s
Bank Acct Info.
Medical Records
TLS Secured Connections
TLS Certificates
Company on the Internet

Risk: Outages

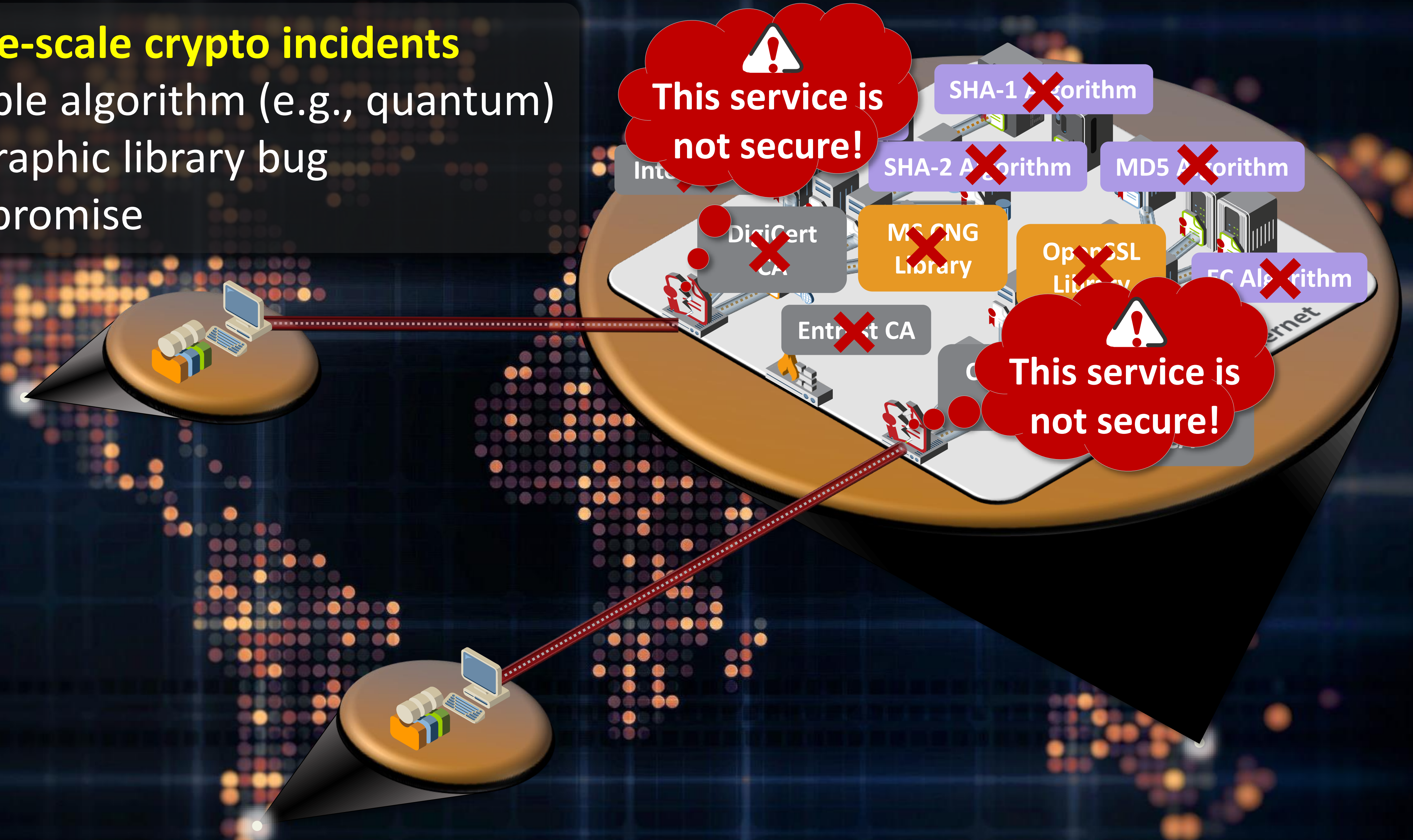


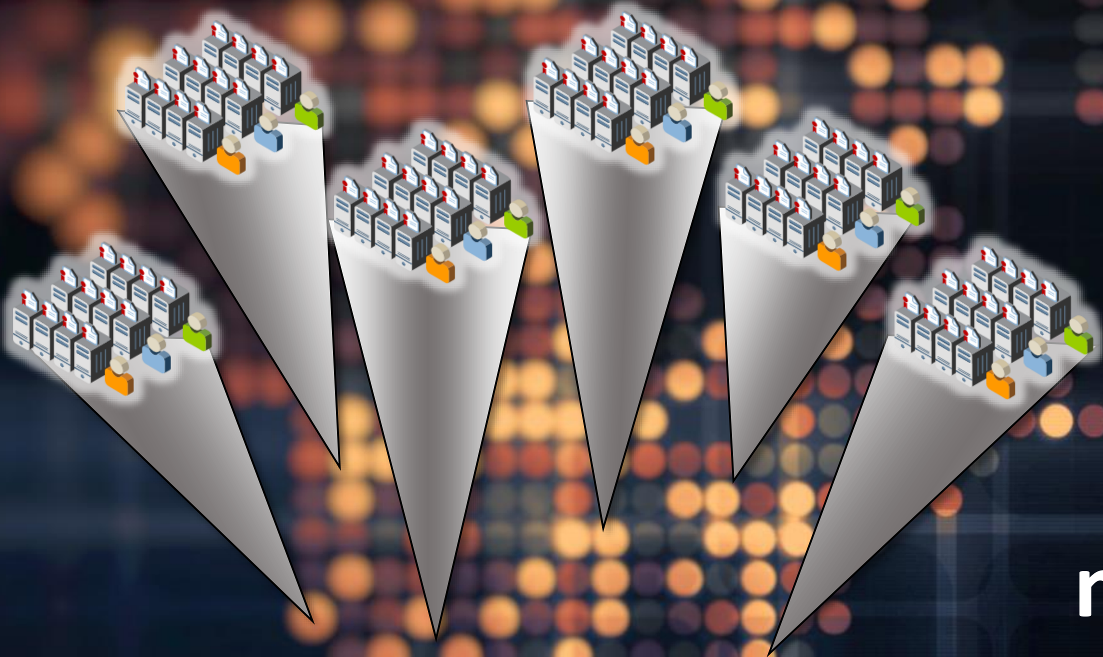
Risk: Encrypted Threats

Company on the Internet

Risk: Large-scale crypto incidents

- Vulnerable algorithm (e.g., quantum)
- Cryptographic library bug
- CA compromise





TLS certificates are spread across many groups/departments, making effective management a challenge.

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Practice Guide Overview

William C Barker

Volume A – Executive Overview

- Brief Overview for Managers
- Description of Challenge
- Description of Solution
- Identification of Collaborators

Volume B - Security Risks and Recommended Best Practices

- New Practice Guide Element: Fills gap in current NIST guidelines
- Identifies project objective and scope
- Background information on server certificates
- Identification of certificate-based risks
- Organization-based challenges
- Recommended best practices
- Suggestions for implementation

Volume C - Approach, Architecture, and Security Characteristics

Overview

- Risk management and security requirements met
- Laboratory architecture and components
- Functional capabilities demonstration design and findings
- Future build considerations

Volume D – How-To Guide

- **Supporting infrastructure**
- **Product installation and configuration instructions**
- **Appendices**
  - Passive inspection
  - Hardening Guidance
  - Underlying concepts

Comments on Drafts

- Editorial
- Visibility
- Certificate revocation

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Summary of Public Comments

Mary Raguso

Public Comments – An Overview

- SP 1800 publications begin with a “project description” which presents the challenge the NCCoE is addressing and is released in draft form to offer the public the opportunity to comment on the contents

- Typically, there are two comment periods—one for the draft and one for the final draft and can last between 30 – 60 days

- Every comment is carefully considered and acknowledged

Public Comments – An Overview

- SP 1800-16, *Securing Web Transactions: Managing Transport Layer Security Server Certificates* has had four comment periods

- We followed an agile process by releasing Volumes A (Executive Summary) and B (Security Risks and Recommended Best Practices) in December 2018 for public comment, and released the full guide in July asking the public to comment again

The Top Five Downloads

The first practice guide in the “NIST Special Publication 1800” series, *Securing Electronic Health Records on Mobile Devices* was released in 2015

Today, there are 24 publications in the SP 1800 series

For the period of December 2018 (when Volumes A&B were released) to August 2018, the top practice guide downloads were:

IT Asset Management (Financial Sector)	7,496
Securing Web Transactions: TLS Sever Certificate Management	**6,819**
Privileged Account Management (Financial Sector)	5,198
Mobile Device Security	3,490
Mitigating IoT-Based DDoS Using Manufacture Usage Description	3,425

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Demonstration

Brett Pleasant, Mehwish Akram, Brian Johnson

Demonstration

Presentation is interactive video based on fictious and troubled mock organization called the WebACME Corporation

Using a bit of your help, the WebACME corporation just may make it through the following incidents:

TLS Certificate Management Security Incidents:

- **Incident 1: Keys to your Heart –** Something really important is missing from WebACME's PKI Infrastructure.
- **Incident 2: The Bad News Bro -** With friends like these, who needs enemies? WebACME's new CEO meets a new friend he doesn't want to know.
- **Incident 3: TLS Terminator 1000 -** Automation has its perks when used for good. Find out why WebACME's missteps in choices for automated services comes back to bite them.
- **Incident 4: Game of Poles – North and South** – If you've watched enough cable TV, then you will know that the north and south have always had wars. What about the man in the middle?
- **Incident 5: Curious Case of the Credit Card -** Guess who is paying for hacker's Christmas presents this year? All of WebACME's customers with credit cards.

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Break!

15 mins

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Andrew Regenscheid

Transport Layer Security

*TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent **eavesdropping, tampering, and message forgery.***

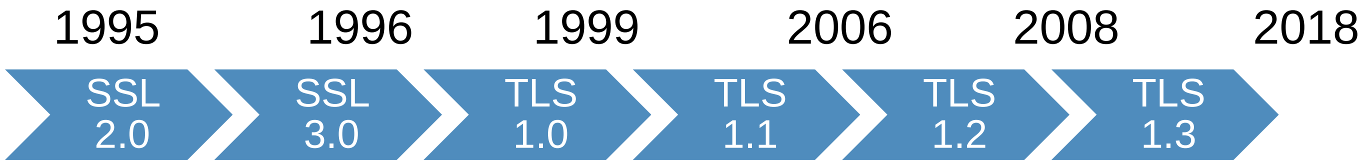
TLS Protocol v1.3 [RFC 8446]

History

- Netscape developed SSL to support e-commerce
- Developed into TLS by IETF

TLS has become the secure protocol of choice

- ~ 80% of web traffic encrypted
- Used with HTTP, SMTP/IMAP, DNS, VPNs, EAP/wifi authentication, etc.



1995 SSL 2.0

1996 SSL 3.0

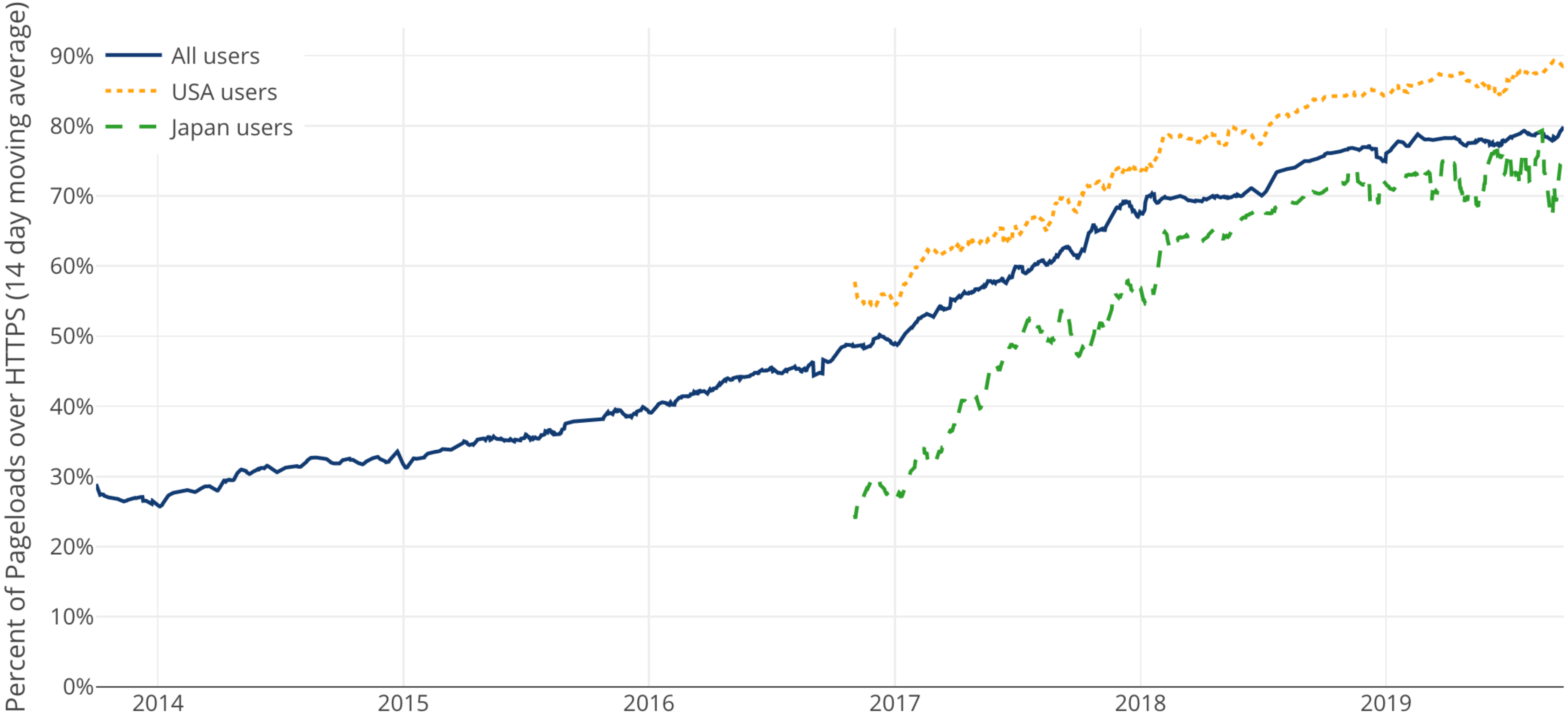
1999 TLS 1.0

2006 TLS 1.1

2008 TLS 1.2

2018 TLS 1.3

Percentage of Web Pages Loaded by Firefox Using HTTPS



Source: Let’s Encrypt and Firefox Telemetry

TLS Security Goals

To provide an authenticated, protected channel between peers

Authentication

- Server identity/domain authenticated (typically) through certificates
- Optional client authentication

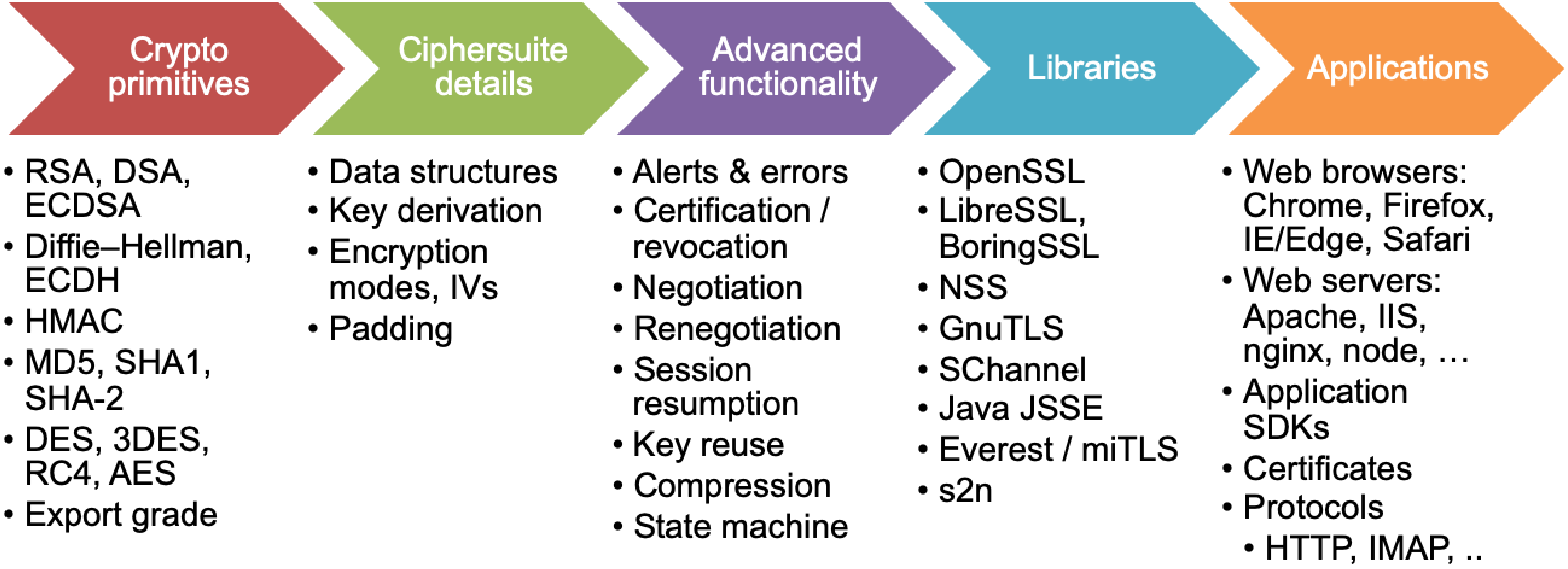
Confidentiality

- Plaintext data is only visible to endpoints

Integrity

- Transmitted data cannot be altered without detection

TLS Components



Crypto primitives

- RSA, DSA, ECDSA
- Diffie–Hellman, ECDH
- HMAC
- MD5, SHA1, SHA-2
- DES, 3DES, RC4, AES
- Export grade

Ciphersuite details

- Data structures
- Key derivation
- Encryption modes, IVs
- Padding

Advanced functionality

- Alerts & errors
- Certification / revocation
- Negotiation
- Renegotiation
- Session resumption
- Key reuse
- Compression
- State machine

Libraries

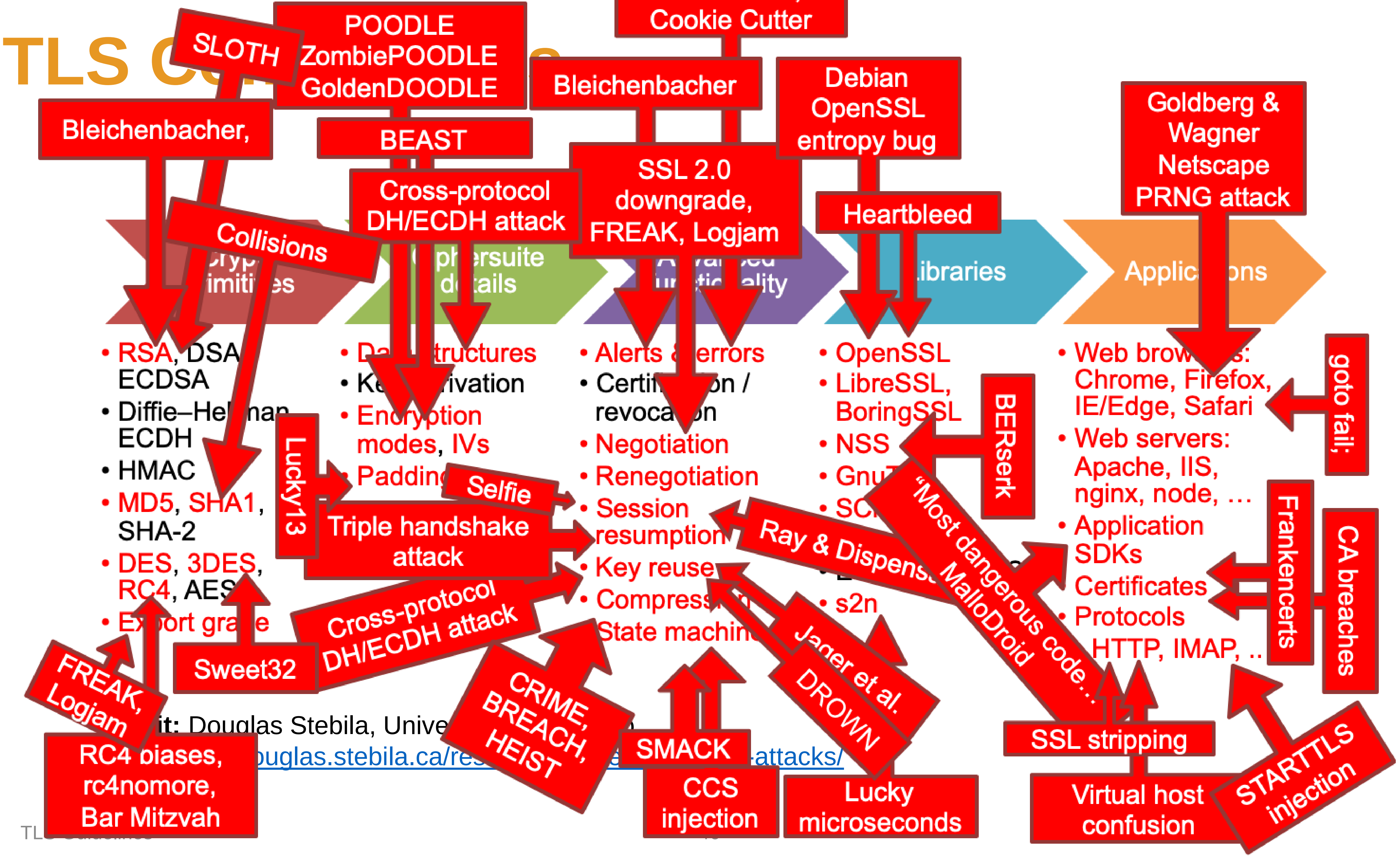
- OpenSSL
- LibreSSL, BoringSSL
- NSS
- GnuTLS
- SChannel
- Java JSSE
- Everest / miTLS
- s2n

Applications

- Web browsers: Chrome, Firefox, IE/Edge, Safari
- Web servers: Apache, IIS, nginx, node, …
- Application SDKs
- Certificates
- Protocols
  - HTTP, IMAP, ..

Credit: Douglas Stebila, University of Waterloo
https://www.douglas.stebila.ca/research/presentations/tls-attacks/

TLS Co



Cryp… imiti…es

- RSA, DSA, ECDSA
- Diffie–Hel…nan, ECDH
- HMAC
- MD5, SHA1, SHA-2
- DES, 3DES, RC4, AES
- Ex…ort gra…e

…phersuite d…ails

- Da… …tructures
- Ke… …rivation
- Enc…yption modes, IVs
- Padding

A…vanced …unctio…ality

- Alerts & errors
- Certi… …on / revoca…on
- Negotiation
- Renegotiation
- Session resumption
- Key reuse
- Compress…
- State machin…

…ibraries

- OpenSSL
- LibreSSL, BoringSSL
- NSS
- Gnu…
- SC…
- …
- s2n

Applic… …ons

- Web brow…s: Chrome, Firefox, IE/Edge, Safari
- Web servers: Apache, IIS, nginx, node, …
- Application SDKs
- Certificates
- Protocols … HTTP, IMAP, ..

SLOTH

POODLE ZombiePOODLE GoldenDOODLE

Cookie Cutter

Bleichenbacher

Debian OpenSSL entropy bug

Goldberg & Wagner Netscape PRNG attack

Bleichenbacher,

BEAST

Cross-protocol DH/ECDH attack

SSL 2.0 downgrade, FREAK, Logjam

Heartbleed

Collisions

goto fail;

BERserk

Lucky13

Selfie

Triple handshake attack

Ray & Dispens…

"Most dangerous code…

MalloDroid

Frankencerts

CA breaches

Cross-protocol DH/ECDH attack

Sweet32

FREAK, Logjam

CRIME, BREACH, HEIST

Jager et al.

DROWN

SMACK

SSL stripping

STARTTLS injection

RC4 biases, rc4nomore, Bar Mitzvah

CCS injection

Lucky microseconds

Virtual host confusion

…it: Douglas Stebila, Unive…

…uglas.stebila.ca/res… …-attacks/

NIST TLS Guidelines

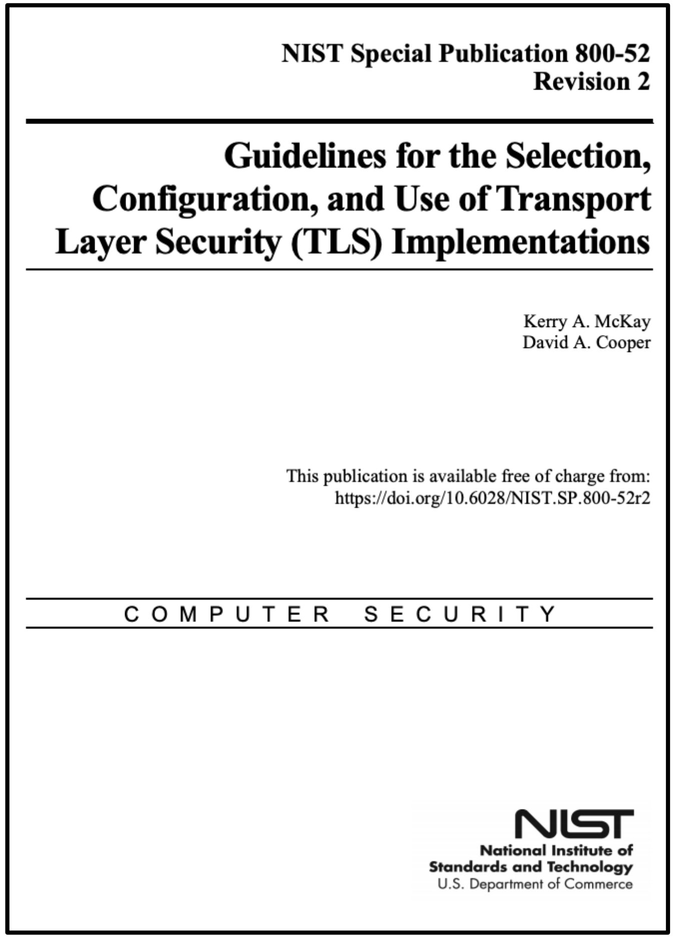
NIST SP 800-52r2, *Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations*

Released August 2019

TLS protocol guidance intended for variety of applications

Topics Covered:

- Server and client implementations
- Protocol version support
- Recommended cipher suites
- Configuration of TLS extensions
- Certificate guidelines



NIST Special Publication 800-52
Revision 2

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Kerry A. McKay
David A. Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-52r2

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

What’s New?

A lot has happened since SP 800-52r1:

New version: TLS 1.3

New Attacks

New cipher recommendations

- NIST deprecating TDEA

New key exchange recommendations

- NIST deprecating RSA key transport that uses PKCS#1_v1.5
- New finite field groups and elliptic curves approved

Government-wide policy changes

- Use TLS on all websites

TLS Version Support

Servers and clients required to support TLS 1.2

- Starting in 2024, also required to support TLS 1.3
- Major browsers disabling TLS 1.0/1.1 in early 2020

Servers that support government-only applications

- ***Should not*** support TLS 1.1
- Not permitted to support TLS 1.0, SSL 2.0, or SSL 3.0

Servers for public-facing applications

- TLS 1.0 and 1.1 ***discouraged***, but may be needed for interoperability
- Not permitted to support SSL 2.0 or SSL 3.0

Recommended Cipher Suites

Any cipher suite that only uses NIST-recommended algorithms and key lengths is acceptable and may be configured

TLS 1.0-1.2 :

- **Key exchange/Signing:** DHE_RSA, ECDHE_RSA, ECDHE_ECDSA, DHE_DSS, ECDH_ECDSA
- **Confidentiality/Integrity:** AES_128_CBC, AES_256_CBC, AES_128_GCM, AES_256_GCM, AES_128_CCM, AES_256_CCM, AES_128_CCM_8, AES_256_CCM_8

TLS 1.3

- **GCM-based:** AES_128_GCM_SHA256, AES_256_GCM_SHA384
- **CCM-based:** AES_128_CCM_SHA256 , TLS_AES_128_CCM_8_SHA256

Deprecated Crypto Algorithms

TDEA/3DES

- Phased out by NIST through 2023
- Not allowed under SP 800-52r2
- 64-bit block ciphers unsuitable for bulk data encryption- *Sweet32 atta*

RSA PKCS#1v1.5

- Legacy key transport
- Prone to implementation flaws- *ROBOT Attack*
- Lacks forward secrecy

DSA-Style DH Groups

- Prone to implementations flaws- *public key validation*
- SP 800-56A recommends use of named IKE/TLS groups

Sweet32
https://sweet32.info

ROBOT Attack
https://robotattack.org

TLS Extensions

TLS Extensions provide additional capabilities and security features, e.g.:

- Elliptic curve crypto extensions
- Supported Groups extension (i.e., named groups)
- Server Name Indication (SNI) and Encrypted SNI (eSNI)
- Certificate Status Request (i.e., OCSP stapling)
- Signed Certificate Timestamps (i.e., Certificate Transparency TLS extension)

NIST SP 800-52r2 provides extension configuration guidance

- *Mandatory, Conditionally required, Discouraged*
- Based on versions and features supported

Example: Early Data Indication (TLS 1.3)

- Known as 0-RTT, allowing client to send data before handshake is complete
- Discouraged due to lack of replay protection

Certificates

Servers need X.509 version 3 certificates

- Optional for clients, used for mutual authentication
- Certificate profiles provided, consistent with industry best practices

At least one certificate needs to be RSA signature certificate or ECDSA signature certificate

- *Signing key length:* ≥ 2048 bit RSA keys or ≥ 256 bit ECDSA keys
- *Hash function:* SHA-2 or SHA-3

Certificate Authority must publish Online Certificate Status Protocol (OCSP) information

- Revocation info can also be obtained from Certificate Revocation Lists
- OCSP Stapling recommended

Server/Client Implementations

Protocol version, cipher suites, TLS extensions support

Certificate Path Validation

- Manage trust anchors
- Revocation Checking
  - Servers/clients should support OCSP stapling

Use Validated Cryptographic Modules

- Approved and tested algorithms
- Assessed RBGs and entropy sources (when available)

Patch! Patch! Patch!

Hearbleed Bug
http://heartbleed.com/

Summary

Risk

- Because of its widespread use online, SSL and TLS have been targets by security researchers and attackers. Many vulnerabilities in SSL and TLS have been uncovered over the past 20 years.

Vulnerability Classes

- Protocol vulnerabilities
- Implementation vulnerabilities
- Configuration vulnerabilities

Impact

- Loss of confidentiality or integrity
- Loss of cryptographic keys

Recommendations

- Migrate to TLS 1.2 and TLS 1.3
- Use strong Cryptography
- Configure TLS securely
- Patch TLS software against implementation vulnerabilities

Questions?

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
UNITED STATES DEPARTMENT OF COMMERCE
100 Bureau Drive

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TLS Project Team Panel Discussion

TLS Project Team Panel Discussion

- **Curt Barker -** NIST
- **Rob Clatterbuck -** Safenet AT
- **Clint Wilson -** Digicert
- **Dung Lam -** F5
- **Jane Gilbert -** Safenet AT
- **Paul Turner -** Venafi

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Optional Lab Tour

Optional TLS Server Certificate Management Lab Tour

- Please wait here in the conference room to be escorted
- TLS Lab Room is: #43
- If you have questions, please ask for help from one of the following:
  - Brett Pleasant
  - Mehwish(Mavish) Akram
  - Brian Johnson

BACKUP SLIDES